Information Security Policy Sample

Aligns with ISO/IEC 27001:2022 Annex A.9 - Access Control and Annex A.10 - Cryptography

Company Name: SecurePath Tech Solutions, Inc.

Policy Title: Access Control and Authenticator Management Policy

Policy ID: ISP-AC-001

Effective Date: 2025-01-01 | **Revision**: 1.0

Policy Owner: Chief Information Security Officer (CISO)

Classification: Internal Use Only

I. Purpose

This policy establishes the requirements for managing access to information systems and ensuring secure authentication mechanisms. The policy aligns with

- ISO/IEC 27001:2022 Annex A.9 - Access Control and
- Annex A.10 - Cryptography.

II. Scope

This policy applies to all employees, contractors, and third-party users accessing HypotheticalTech information systems.

III. Policy Statements

- Access to information and systems shall be granted on a least-privilege basis
- User access rights must be reviewed quarterly by system owners
- Multi-factor authentication (MFA) is mandatory for all privileged accounts
- All user accounts must have unique identifiers and secure password controls
- Shared or generic accounts are prohibited unless approved by the CISO

IV. Roles and Responsibilities

- IT Security Team: Enforce technical controls and review audit logs
- Department Heads: Validate and authorize user access requests
- All Users: Adhere to this policy and report violations

V. Compliance and Enforcement

Non-compliance with this policy may result in disciplinary actions, including termination of access privileges or employment. Exceptions must be documented and approved by the CISO.